



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/282,633	03/31/1999	CHRISTIAN LITA	AT9-99-088	8871

7590 09/30/2002

LAW OFFICES OF JOSEPH R BURWELL
P O BOX 28022
AUSTIN, TX 78755-8022

EXAMINER

MOORTHY, ARAVIND K

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 09/30/2002

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/282,633

Applicant(s)

LITA ET AL.

Examiner

Aravind K Moorthy

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) 10-25 is/are allowed.
- 6) ☐ Claim(s) 1 and 3-9 is/are rejected.
- 7) ☐ Claim(s) 2-5 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on 11 March 1999 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on ____ is: a) ☐ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. The detailed description of the claimed invention lacks patentable utility. On page 8 lines 14-15, of the specifications, the applicant discloses that any given program may be capable of being both a client and a server. The examiner asserts that not every program is capable of being both a client and a server. Not all games and applications are capable of being a client or server.

3. Specification

4. The disclosure is objected to because of the following informalities: typographical error. On page 10 and line 20 of the specifications, applicant put "FLS" instead of "TLS".

Appropriate correction is required.

5. Drawings

6. Figures 1 and 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). In figure 1, the connection between a client and server using SSL or TLS is not new to the art. In figure 2, the use of a proxy between a client and server with a SSL or TLS connection is not new to the art. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Art Unit: 2131

7. Claim Objections

8. Claims 2-5 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Prior art does not teach the step of having a proxy use a session master secret and a session identifier to generate cryptographic information.

9. Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 3-5 and 11-13 are rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. Details critical or essential to the practice of the invention, but not included in the claim(s) is not enabled by the disclosure. See *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976). Applicant discloses the proxy entering an active operating state following receipt of the session master secret and generation of the given cryptographic information. There are not enough details in the specification for the examiner to understand how the proxy enters an active operating state following receipt of the session master secret and generation of the given cryptographic information. The examiner asserts that the proxy should already be in an active operating state to receive a session master secret and generate any given cryptographic information.

Any claims not addressed are rejected on the virtue of dependency.

11. Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

12. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vu U.S. Patent No. 5,623,601 in view of Raivisto U.S. Patent No. 6,081,601.

As per claim 1, Vu discloses establishing a first secure connection between the client and the proxy (gateway station 14). Vu discloses that upon verifying the first secure session, establishing a second secure session between the client and the proxy (gateway station 14), the second secure session requesting the proxy to act as a conduit to the server, column 8 lines 54-64. Vu does not disclose having the client and the server negotiate a session master secret and delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication.

The examiner asserts that is obvious that there is no direct connection between the client and server therefore the secret between the client and the server is going to go through the proxy server. Microsoft Computer Dictionary defines a proxy as a computer (or software that runs on it) that acts as a barrier between a network and the Internet by presenting only a single network address to external sites. And by acting as a go-between representing all internal computers, the proxy protects network identities while still providing access to the Internet. So any secret going from the client to the server has to go through the proxy.

Raivisto's invention relates to a method of providing connection security for a connection between terminals in a wireless network. Data is routed via a mediator (**MD**), that is going to serve as the proxy; using the first security method for providing connection security at the security protocol layer between the first terminal (**MS1**) and the mediator (**MD**), using the second security method for providing connection security at the security protocol layer between the mediator (**MD**) and the second terminal (**MS2**), and performing the security method conversion at the security protocol layer at the mediator (**MD**), see abstract. Raivisto discloses that the first cryptographic key **K1** can be the public key of the mediator used in a public key algorithm or a secret key shared between **MS1** and the mediator **MD** and used in a symmetric ciphering algorithm, column 4 lines 60-64. The second cryptographic key **K2** can be the public key of **MS2** used in a public key algorithm or a secret key shared between the mediator **MD** and **MS2** and used in a symmetric ciphering algorithm.

The advantage of the method according to the invention is that the management of keys and other parameters needed for connection security is simple and secure. When applying this method, only a few security parameters need to be stored at mobile terminals. Another advantage of the method according to the invention is that mobile terminals using incompatible security algorithms and/or security layer protocols can communicate with each other with the connection security provided.

Vu's invention applied with Raivisto is a system with a secure a connection and efficient key management. A first secure connection will be made between a client (**MS1**) and a proxy (**MD**). A second connection will be made between a client (**MS1**) and a proxy (**MD**) that

Art Unit: 2131

enables the proxy to act as a conduit to the server. Secret keys will be established the proxy (MD) and the client (MS1) and the proxy (MD) and the server (MS2).

13. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vu U.S. Patent No. 5,623,601 and Raivisto U.S. Patent No. 6,081,601 as applied to claim 1 above, and further in view of Davis et al U.S. Patent No. 6,367,009.

The examiner asserts that it is obvious to use the network security protocol of SSL. SSL is designed to be an extensible protocol, so that new record types can be introduced without requiring creation of a new protocol (which introduces new security weaknesses), column 10 lines 52-64.

The examiner asserts that TLS can be used in place of SSL. One of ordinary skill in the art can substitute SSL with TLS. TLS specification is designed as a follow-on security technique that will replace SSL. SSL will end with Version 3.0 and TLS will begin with a Version 1.0 that is based on the SSL Version 3.0 specification, column 9 line 66 through column 10 lines 1-18.

14. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vu U.S. Patent No. 5,623,601 and Raivisto U.S. Patent No. 6,081,601 as applied to claim 1 above, and further in view of Rosecrans et al U.S. Patent No. 5,889,852.

As defined by the applicant in the specifications on pages 1 and 2, a "pervasive computing" client is a device that is designed to be connected to servers in a computer network and used for computing purposes regardless of their location. Examples of "pervasive computing" clients are listed on page 1 and they can devices such as: personal digital assistants (PDAs), business organizers (e.g. IBM® Work Pad® and the 3Com® Palm Pilot®), smart phones, cellular phones, other handheld devices, and the like.

The Vu and Raivisto combination uses cellular phones. As shown in figures 5, 6, 8 and 9 of Raivisto, MS1-MS4 are cellular phones which are, as defined by the applicant, "pervasive computing" clients. As for the server being a web server, the examiner asserts that it is obvious that a cellular phone can be a web server.

Newton's Telecom Dictionary defines web server as a powerful computer that is connected to the Internet or an Intranet. It stores documents and files-audio, video, graphics or text-and can display them to people accessing the server via hypertext transfer protocol (http).

Neither Vu nor Raivisto disclose the server as being a web server. Rosecrans et al discloses a graphic user interface, for use with electronic phonebooks, links graphic information, e.g. a graphic identifier such as a logo or picture, to a phone number that may be called using the graphic identifier. The interface, incorporated in a telephone, enables users to send stored graphical information, tied to selected numbers, to other users' phones for use or storage, by scrolling through stored graphics, displayed by the interface on the phone, to locate a graphic associated with a person or place to be called, and then, by pressing SEND, the particular phone number or numbers linked to the selected graphic are activated and the call or calls are made, see abstract.

This feature added to the phones in the Vu-Raivisto provides the cellular phones with a capability that allows the user to tie a picture, icon, or other graphical representation to a person, place, or entity so that recognition can be quick and easy and the icon may be used to initiate a phone call to the tied person.

15. Allowable Subject Matter

16. Claims 10-25 are allowed.

As per claim 10, prior art does not disclose the proxy using the session master secret and the session identifier to generate given cryptographic information that is useful for participating in the secure communication.

As per claim 17, prior art does not disclose conducting a security handshake procedure between the client and the server to produce a session key and transmitting the session key to the proxy so that the proxy can participate in communications between the client and the server during the session.

As per claim 18, prior art does not disclose the session key being transmitted from the client to the proxy over a secure connection.

As per claim 20, prior art does not disclose upon successful completion of the negotiation, controlling the client to deliver the session master secret to the proxy using the first secure connection. Prior art also does not teach a computer program for controlling the proxy to use the session master secret and a session identifier to cryptographic information.

Any claims not addressed are allowed on the virtue of dependency

17. Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes can be reached on 703-305-9711. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-7239 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

September 26, 2002


GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100